

Revised February 24, 2020

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

ZACHARY NERO, et al.,

Plaintiffs,

against

UPHOLD HQ INC., et al.

Defendants.

CIVIL ACTION NO.: 1:22 Civ. 01602 (DLC)

**MODEL CONFIDENTIALITY STIPULATION  
AND PROPOSED PROTECTIVE ORDER**

**WHEREAS**, the Parties having agreed to the following terms of confidentiality, and the Court having found that good cause exists for the issuance of an appropriately tailored confidentiality order pursuant to Rule 26(c) of the Federal Rules of Civil Procedure, it is hereby

**ORDERED** that the following restrictions and procedures shall apply to the information and documents exchanged by the parties in connection with the pre-trial phase of this action:

1. Counsel for any party may designate any document or information, in whole or in part, as confidential if counsel determines, in good faith, that such designation is necessary to protect the interests of the client in information that is proprietary, a trade secret or otherwise sensitive non-public information. Information and documents designated by a party as confidential will be stamped "CONFIDENTIAL."

2. The Confidential Information disclosed will be held and used by the person receiving such information solely for use in connection with the action.

3. In the event a party challenges another party's designation of confidentiality, counsel shall make a good faith effort to resolve the dispute, and in the absence of a resolution, the challenging party may seek resolution by the Court. Nothing in this Protective Order constitutes an admission by any party that Confidential Information disclosed in this case is relevant or admissible. Each party reserves the right to object to the use or admissibility of the Confidential Information.

4. The parties should meet and confer if any production requires a designation of "For Attorneys' or Experts' Eyes Only." All other documents designated as "CONFIDENTIAL" shall not be disclosed to any person, except:

- a. The requesting party and counsel, including in-house counsel;
- b. Employees of such counsel assigned to and necessary to assist in the litigation;

- c. Consultants or experts assisting in the prosecution or defense of the matter, to the extent deemed necessary by counsel; and
- d. The Court (including the mediator, or other person having access to any Confidential Information by virtue of his or her position with the Court).

5. Prior to disclosing or displaying the Confidential Information to any person, counsel must:

- a. Inform the person of the confidential nature of the information or documents;
- b. Inform the person that this Court has enjoined the use of the information or documents by him/her for any purpose other than this litigation and has enjoined the disclosure of the information or documents to any other person; and
- c. Require each such person to sign an agreement to be bound by this Order in the form attached as Exhibit A.

6. The disclosure of a document or information without designating it as "Confidential" shall not constitute a waiver of the right to designate such document or information as Confidential Information. If so designated, the document or information shall thenceforth be treated as Confidential Information subject to all the terms of this Stipulation and Order.

7. Any Personally Identifying Information ("PII") (e.g., social security numbers, financial account numbers, passwords, and information that may be used for identity theft) exchanged in discovery shall be maintained by the receiving party in a manner that is secure and confidential and shared only with authorized individuals in a secure manner. The producing party may specify the minimal level of protection expected in the storage and transfer of its information. In the event the party who received PII experiences a data breach, it shall immediately notify the producing party of same and cooperate with the producing party to address and remedy the breach. Nothing herein shall preclude the producing party from asserting legal claims or constitute a waiver of legal rights and defenses in the event of litigation arising out of the receiving party's failure to appropriately protect PII from unauthorized disclosure.

8. Pursuant to Federal Rule of Evidence 502, the production of privileged or work-product protected documents or communications, electronically stored information ("ESI") or information, whether inadvertent or otherwise, shall not constitute a waiver of the privilege or protection from discovery in this case or in any other federal or state proceeding. This Order shall be interpreted to provide the maximum protection allowed by Federal Rule of Evidence 502(d). Nothing contained herein is intended to or shall serve to limit a party's right to conduct a review of documents, ESI or information (including metadata) for relevance,

responsiveness and/or segregation of privileged and/or protected information before production.

9. Notwithstanding the designation of information as "Confidential" in discovery, there is no presumption that such information shall be filed with the Court under seal. The parties shall follow the Court's procedures for requests for filing under seal.

10. At the conclusion of litigation, Confidential Information and any copies thereof shall be promptly (and in no event later than 30 days after entry of final judgment no longer subject to further appeal) returned to the producing party or certified as destroyed, except that the parties' counsel shall be permitted to retain their working files on the condition that those files will remain protected.

11. Nothing herein shall preclude the parties from disclosing material designated to be Confidential Information if otherwise required by law or pursuant to a valid subpoena.

SO STIPULATED AND AGREED.

Dated: New York, New York

April 20, 2023

4/21/23

SO ORDERED.

SARAH E. CAVER  
Sarah E. Caver  
United States Magistrate Judge

Exhibit A

Agreement

I have been informed by counsel that certain documents or information to be disclosed to me in connection with the matter entitled have been designated as confidential. I have been informed that any such documents or information labeled "CONFIDENTIAL" are confidential by Order of the Court.

I hereby agree that I will not disclose any information contained in such documents to any other person. I further agree not to use any such information for any purpose other than this litigation.

DATED:

---

Signed in the presence of:

---

(Attorney)

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK**

ZACHARY NERO, JESSE W. SMITH,  
PETER MALOUPIS, JOSÉ RAMIREZ, and  
GILLES BOEVI, individually and on behalf  
of other similarly situated individuals,

Plaintiffs,

v.

UPHOLD HQ INC., a South Carolina  
corporation, JUAN PABLO THIERIOT, aka  
J.P. THIERIOT, an individual, and JOHN  
DOES 1–10, individuals,

Defendants.

Civil Action No. 1:22-cv-01602

**STIPULATED ORDER RE: DISCOVERY  
OF ELECTRONICALLY STORED  
INFORMATION**

**1. PURPOSE**

This Order will govern discovery of electronically stored information (“ESI”) in this case as a supplement to the Federal Rules of Civil Procedure, this Court’s Guidelines for the Discovery of Electronically Stored Information, and any other applicable orders and rules.

**2. COOPERATION**

The parties are aware of the importance the Court places on cooperation and commit to cooperate in good faith throughout the matter consistent with this Court’s Guidelines for the Discovery of ESI.

**3. PRESERVATION**

The parties have discussed their preservation obligations and needs and agree that preservation of potentially relevant ESI will be reasonable and proportionate. To reduce the costs and burdens of preservation and to ensure proper ESI is preserved, the parties agree that:

- a) Only ESI created or received since January 1, 2019 will be preserved;
- b) The parties will agree on the number of custodians per party for whom ESI will be preserved;

#### **4. SEARCH**

The parties agree that in responding to an initial Fed. R. Civ. P. 34 request, or earlier if appropriate, they will meet and confer about methods to search ESI in order to identify ESI that is subject to production in discovery and filter out ESI that is not subject to discovery. This does not require, however, that the parties must disclose or agree on the precise search terms to be used in locating responsive documents in the first instance.

#### **5. PRODUCTION FORMATS**

a. TIFF Images. Unless otherwise stated in this Production Protocol, each document shall be produced in black and white, CCITT Group IV Tagged Image File Format (“TIFF”) regardless of whether such documents are stored by the parties in the ordinary course of business in electronic or hard copy form. Each TIFF image file should be one page and should reflect how the source document would appear if printed to hard copy.

b. Load File(s). Document productions shall include Concordance-compatible Load File(s) that indicates document breaks of the TIFF images and additional fields as identified in Section 8 below.

c. File Name. Each document image file shall be named with the unique Bates Number of the first page of the document in question followed by the file extension “TIF”. File names should not be more than fifteen characters long or contain spaces or underscore symbols.

d. Document Unitization. Electronically collected data shall maintain family relationships to group parent documents with their attachments. Parties shall apply all appropriate measures to logically unitize any hard copy or scanned documents in order to represent how they were maintained in the ordinary course of business.

e. Color. Documents shall be produced as black and white TIFF images. Upon written request, a party shall produce color images for a reasonable number of selected documents. Documents produced in color shall be produced as JPEG images with Exif compression and 24-bit color depth. Each color document image file shall be named with the

unique Bates Number of the first page of the document in question followed by the file extension “JPG”.

f. Confidentiality Designation. Responsive documents in TIFF format will be stamped with the appropriate confidentiality designations in accordance with the Protective Order in this matter. Each responsive document produced in native format will have its confidentiality designation identified in the filename of the native file.

g. Native Production for Spreadsheets, PowerPoint Presentations, and other Files not readily converted into TIFF images. Notwithstanding the foregoing, the parties will produce spreadsheet and PowerPoint and other presentation files in native format, as well as any other files not readily converted into a TIFF image (e.g., audio or video files). Each file produced in native format shall be named with a unique Bates Number (*e.g.*, ABC00000001.xls) and protective designation (*e.g.* ABC00000001\_confidential.xls). In addition to producing such documents in native format, the producing party shall also include in the production a placeholder TIFF image with the phrase “Document Produced Natively.” The placeholder TIFF images shall be Bates-numbered as described herein, shall be endorsed for confidentiality as described in the Protective Order, and shall include Metadata as set forth in Section 8. The parties reserve the ability to request other file types be produced in native form or in another reasonably usable form upon review of the other party’s production. The parties reserve their respective rights to object to any such request

h. Native Redactions. Spreadsheets that contain redactions shall be produced as TIFF images, and shall follow the TIFF-image protocol described herein. However, when reasonably necessary, large spreadsheets that contain redactions may be produced in native format with black boxes representing the redacted portions of the document. These documents shall be redacted using a “full block” representative character that appears as a black box on the spreadsheet. This process may be used when a TIFF image would otherwise result in a large number of pages such that it is unreasonable to review as a TIFF image.

## **6. SEARCHABLE TEXT**

In addition to TIFF images, each production will include text files corresponding to the TIFF image files described above.

a. Hard Copy Documents. Hard copy documents shall be scanned using Optical Character Recognition (“OCR”) technology and searchable ASCII text (or Unicode text if the text is in a language requiring characters outside of the ASCII character set) files shall be produced. Each file shall be named with the unique Bates Number of the first page of the corresponding TIFF document followed by the extension “TXT”. Hard copy documents shall otherwise be produced as they are stored in the normal course of the producing party’s business.

b. Electronic Documents. The full text of each native electronic document shall be extracted (“Extracted Text”) and produced in a text file. The Extracted Text shall be provided in searchable ASCII text format (or Unicode text format if the text is in a language requiring characters outside of the ASCII character set) and shall be named with the unique Bates Number of the first page of the corresponding TIFF document followed by the extension “TXT”. Searchable text files corresponding to the TIFF image files for redacted Electronic Documents must include Extracted Text or OCR text only to the extent that it will not disclose redacted information.

## **7. PRODUCTION MEDIA**

Documents that are designated pursuant to the protective order must be produced via encrypted media or via encrypted FTP transfer or other securely encrypted electronic transmissions. Each FTP production transfer and piece of Production Media shall identify: (1) the producing party’s name; (2) the production date; and (3) the Bates Number range of the materials contained on the Production Media.

## **8. METADATA**

a. For all Electronic Documents, the Concordance compatible Load File(s) referenced in paragraph 5(b) will be in an ASCII text format and include the Data Fields listed

below. For redacted Electronic Documents, metadata fields must be produced only to the extent such fields will not disclose redacted information.

b. The parties reserve the ability to request that additional Data Fields be set forth or provided for certain specified Electronic Documents upon review of the other party's production. A party is not obligated to produce metadata from a document if metadata does not exist in the document, is not machine-extractable, or is otherwise not reasonably available. Notwithstanding, the Custodian and Hash Value fields identified below are derived or additive metadata which the parties must produce even though not otherwise existing in the document or machine-extractable.

<b>Field</b>	<b>Field Name</b>	<b>Field Format</b>	<b>Description</b>
Confidentiality	Confid	Text	Confidentiality designation pursuant to the parties' Protective Order
File Name	FileName	Text	File Name of document or email
File Size	FileSize	Text	File size of document or email (including any embedded attachments)
Document Page Count	PageCount	Non zero filled number	Number of pages in email or document
Production Begin Bates Number	BegDoc	Maximum six-character alpha prefix, seven-digit numeric sequence	Document ID number associated with first page of email or document
Production End Bates Number	EndDoc	Maximum six-character alpha prefix, seven-digit numeric sequence	Document ID Number associated with last page of email or document
Production Begin Attachment Bates Number	BegAtta	Maximum six-character alpha prefix, seven-digit numeric sequence	Document ID Number associated with first page of parent email, document or family
Production End Attachment Bates Number	EndAtta	Maximum six-character alpha prefix, seven-digit numeric sequence	Document ID Number associated with last page of email, document or family
Parent ID	ParentID	Maximum six-character alpha prefix, seven-digit numeric sequence	Starting Bates number of Parent document

Attach IDs	AttachIDs	Maximum six-character alpha prefix, seven-digit numeric sequence	Starting Bates number of each attached document separated by semi-colon
Attach Count	AttachCount	Number	Tally of the number of attachments per document
File Type	DocType	Text	Type of file (e.g., email, attachment, network document)
Original File Path	OrigPath	Text	Complete original file path for an email or loose electronic document
File Extension	FileExt	Text	File extension of document or email
Full Text Path	TextPath	Text	UNC path to production text files containing the extracted or OCR text (Not required if text of document is redacted)
MD5/SHA1	MD5Hash/ Secure Hash	Hash value	Algorithm that represents a unique value of the document or email, used for deduplication purposes
Native Link	Native Link	Text	Complete file path of produced native file to allow hyperlinking of native file. (Only if native file is being produced)
Redacted Document	RedctDoc	Y/N	If a document is redacted, this field must contain a "Y." If the document has not been redacted, the field must contain an "N."
Custodian	DocCust	Text	Name of the custodian or source system from which the document was collected.
Duplicate Custodian <sup>1</sup>	DupCust	Text semicolon delimited	List of custodian names that had duplicates of this email or document. Names shall be delimited by a semicolon. Only applicable when the parties use global deduplication.

<sup>1</sup> Global Deduplication is the recommended processing standard for most matters. The Parties shall attempt to de-duplicate ESI to avoid substantially duplicative productions. Documents will be de-duplicated against the entire population and all custodians of a de-duplicated document will be listed in a "Duplicate Custodian" field.

Author	Author	Text	Document author name, for non-email documents.
From	Sender	Text	Name and/or email address of person(s) found in the "FROM" address line.
To	Recipient	Text semicolon delimited	Name(s) and/or email addresses of person found in the "TO" address line.
CC	CC	Text semicolon delimited	Name(s) and/or email addresses of person(s) found in the "CC" address line.
BCC	BCC	Text semicolon delimited	Name(s) and/or email addresses of person(s) found in the "BCC" address line, if any.
Subject	Subject	Text	Subject or "Re" line of email; not required for documents if subject or re line is redacted.
Title	Title	Text	Title of non-email document; not required if title is redacted.
Date Created	CreateDate	Date in MMDDYYYY	Date on which the document was created
Time Created	CreateTime		Time file created
Last Modified Date	DateMod	Date in MMDDYYYY	Date the document was last modified
Last Modified Time	ModTime		Time file last modified
Last Access Date	AccessDate	Date in MMDDYYYY	Date file last accessed
Last Access Time	AccessTime		Time file last accessed
Sent Date	DateSent	Date in MMDDYYYY	Date email was sent
Sent Time	TimeSent		Time email was sent
Date Received	DateRecd	Date in MMDDYYYY	Date email was received by addressed recipients
Time Received	TimeRecd		Time email was received

## **9. EMAIL THREADING**

In order to reduce the volume of entirely duplicative content within email threads, a party may utilize email thread suppression. As used in this agreement, email thread suppression means reducing redundant production of lesser inclusive email threads by producing the most recent email containing the thread of emails, as well as any emails with unique attachments within the thread. Thus excluding all lesser inclusive emails that would constitute redundant duplicates within the produced string. Emails suppressed under this paragraph need not be reflected on the party's privilege log.

## **10. PRIVILEGED DOCUMENTS**

a. For each document withheld on the basis of privilege, the parties agree to include such document on a furnished log that complies with the legal requirements under federal law, but at a minimum will include the following information:

- i. A unique number for each entry on the log.
- ii. The date of document. The parties should indicate what the date of the document signifies. For example, this could be the sent date of the document or the last-modified or create date of the document.
- iii. The Author of the document. For emails this should be populated with the metadata extracted from the “Email From” field associated with the file. For loose ESI, this should be populated with the metadata extracted from the “Author” field; if such field contains generic information such as the company name, a party may substitute the information contained in the “Custodian” metadata field.
- iv. Recipient(s) of the document where reasonably ascertainable. For emails this should be populated with the metadata extracted from the “Email To” field associated with the file. Separate columns should be included for the metadata extracted from the “Email CC” and “Email BCC” fields, where populated.

- v. To the extent the fields identifying the author, sender, and recipient(s) contain counsel, the parties shall bold the names of those counsel so that they are readily identifiable.
  - vi. The fields identifying the sender and recipient(s) of purportedly privileged email communications shall identify the name of the author, sender, and recipient(s) as well as the email addresses of such persons.
  - vii. A description of why privilege is being asserted over the document. This description should include information sufficient to identify if the document contained attachments over which privilege is also being asserted. To the extent the counsel who is the basis of the privilege or work product claim is not apparent from the other information (to, from, cc, etc.) the parties shall identify the attorney(s) in the description.
  - viii. The type of privilege being asserted: (a) AC for Attorney/Client, (b) WP for Attorney Work Product, (c) CI for Common Interest.
- b. The parties shall provide privilege logs and updated privilege logs within 30 days of any substantial production.
- c. Pursuant to Fed. R. Evid. 502(d), the production of a privileged or work-product-protected document, whether inadvertent or otherwise, is not a waiver of privilege or protection from discovery in this case or in any other federal or state proceeding. For example, the mere production of privileged or work-product-protected documents in this case as part of a mass production is not itself a waiver in this case or in any other federal or state proceeding.
  - d. Communications involving trial counsel that post-date the filing of the complaint need not be placed on a privilege log.

## **11. MODIFICATION**

This Stipulated Order may be modified by a Stipulated Order of the parties or by the Court for good cause shown.

**IT IS SO STIPULATED**, through Counsel of Record.

Attorneys for Plaintiffs:

**KRONENBERGER ROSENFELD, LLP**

/s/ Karl S. Kronenberger

Karl S. Kronenberger (NY Bar No. 4631578)  
Katherine E. Hollist (admitted *pro hac vice*)  
150 Post Street, Suite 520  
San Francisco, CA 94108  
Telephone: (415) 955-1155  
Facsimile: (415) 955-1158  
karl@kr.law  
kate@kr.law

Attorneys for Defendant:

**MEISTER SEELIG & FEIN PLLC**

/s/ Benjamin D. Bianco

Benjamin D. Bianco, Esq.  
Caitlin R. Trow, Esq.  
125 Park Avenue, 7th Floor  
New York, New York 10017  
Tel: (212) 655-3500  
Fax: (212) 655-3535  
bdb@msf-law.com  
crt@msf-law.com

DATED: April 21, 2023

SO ORDERED.

Denise L. Cote  
**Denise L. Cote**  
United States District Judge